DYJIX.EU

Dyjix Customer User Guide

Table of contents

I. Overview

Thank you for selecting Dyjix as your Internet service provider!

The Dyjix Customer User Guide has been carefully crafted to address any inquiries that might come up regarding your Dyjix network services. Whether you have an inquiry about setup, upkeep, or client assistance, you'll discover the Dyjix User Guide to be an invaluable comprehensive resource for the information you require. We recommend going through the User Guide in its entirety; however, each section is designed to be self-sufficient, enabling you to quickly locate answers on specific topics.

Our goal

Dyjix's goal is to simplify the delivery process and lower the costs related to high-bandwidth Internet access and/or transportation services. We accomplish this by providing dedicated broadband access to businesses, avoiding oversubscription.

Our network

Here at Dyjix, we deliver a service that merges optical technologies with Internet protocols, ensuring dependable Internet services ranging from 100 Mbps to 100 Gbps. With our ownership and management of the network, you gain from the complete authority we wield over service quality and costs.

II. Default configuration

10G / 40G / 100G configurations :

- Auto negotiation : off
- If Layer 2, IEEE 802.1q VLAN tags will be provided to you if required.

III. Router policy

Dyjix requires all of its customers with a /24 IPv4, /48 IPv6 or larger to have a router, this allows Dyjix to improve its monitoring and provide better support.

IV. Monitoring

When a customer employs a switch and one of the host machines experiences downtime, whether it's planned or unplanned, the connection may appear as down even if the other servers are operational. However, with a router, Dyjix promptly detects the inaccessibility of the customer. As a result, routers offer improved accuracy in diagnosing issues, leading to more effective customer support.

To ensure that Dyjix can uphold the Guarantees and Service Credits outlined in any Service Level Agreement, it is essential to grant access to our monitoring systems, allowing them to reach the monitored host, whether it's your router interface or host IP. The IP addresses used by Dyjix's monitoring systems fall within the range mentioned in the table below.

Region	IPv4 Monitoring Range	IPv6 Monitoring Range
All	185.171.202.178/32	2a10:4640:1::/112

V. DNS Service

If you wish for Dyjix to serve as the primary name server for one or multiple of your domains, it is required that Dyjix is designated as the technical contact for the respective domain(s). When registering domains through Network Solutions, kindly input the designated NIC Handle, "AH13495-RIPE," within the technical contact information sections. In cases where a registry service does not acknowledge this NIC Handle, please provide the subsequent details specifically for the technical contact (excluding the billing contact and domain owner) :

DYJIX SAS
149 AVENUE DU MAINE, 75014 PARIS, FRANCE

E-mail : support@dyjix.eu
Tel : +33 1 89 16 28 08

In this situation, you will also need to provide to the registry the names and IP addresses of Dyjix's primary and secondary name servers.

All regions	IPv4	IPv6
Primary DNS Hostname	ipdns1.dyjix.eu	ipdns1.dyjix.eu
Primary Server Address	185.171.202.251	2a10:4640::2
Secondary DNS Hostname	ipdns2.dyjix.eu	ipdns2.dyjix.eu
Secondary Server Address	185.171.202.253	2a10:4640::3

VI. Blackhole

The BGP community of 65535:666, also known as the blackhole community, facilitates the null-routing of a specific IP address in the event of a DDoS attack.

Please note that Dyjix does not warrant or guarantee that use of the blackhole community will mitigate, or minimize any effects of a DDOS attack.

You can only blackhole IPs addresses with a /32 for IPv4 and /128 for IPv6, and you are limited by the value of max-prefixes indicated on the BGP session. Data is pulled from the PeeringDB site, if failing, default value is 50.

By default, Dyjix implements automatic blackhole thresholds corresponding to the capacity of the client port. To raise or lower these thresholds, contact support.

VII. Customer BGP Informations

- Dyjix operate 32 bits ASN 212815.
- Dyjix support BFD if needed, please ask support at support@dyjix.eu
- Dyjix filters BGP announcements from the customer AS-SET/ASN, based on ROA and RPKI values. The filters are automatically refreshed every day at 6am CET.
- Dyjix puts a maximum prefix value on each BGP session, corresponding to the value indicated in PeeringDB, otherwise the default value is 50.
  If exceeded, the session will be automatically shutdown and will be reactivated after 60 minutes.
- Communities can pass through Dyjix to its upstreams and peering partners, excluding 65500:* communities.
- Dyjix drop invalid routes if RPKI is invalid.

VIII. Services & Features

Our upstreams and peering partners are designed as follow :

Community	Upstream / Peering
65500:1000	Fiberway
65500:1010	FranceIX Route Server
65500:1020	FranceIX Private Peering
65500:1030	Appliwave
65500:1040	FNCIX
65500:1050	FNCIX Private Peering

Our customers are designed as follow :

Community	Upstream / Peering
65500:10000	Customers

Local preference

All customers routes advertised to Dyjix have a default local preference of 199.

Customers can control the local preference for their announcements using a BGP community. The following table describes the different possibilities:

Community	Local Pref	Effect
65500:50	50	Set customer route local preference to 50 (below everything-least preferred)
65500:60	60	Set customer route local preference to 60 (below peers)
65500:150	150	Set customer route local preference to 150 (below customer default)
65500:200	200	Set customer route local preference to 200 (above customer default)

Prepending Communities

These communities affect the actions that Dyjix will take on the routes before sending them to upstream and peering partners :

Community	Effect
65500:1	Prepend 1 time to all peers
65500:2	Prepend 2 time to all peers
65500:3	Prepend 3 time to all peers

We also support prepending per upstream or per peer. You must use communities described into “**Our upstreams and peering partners are designed as follow**” and replace “**1**”, “**2**”, “**3**” on the last number, some examples :

Community	Effect
65500:1001	Prepend 1x to Fiberway
65500:1002	Prepend 2x to Fiberway
65500:1003	Prepend 3x to Fiberway
65500:1011	Prepend 1x to FranceIX Route Server
65500:1012	Prepend 2x to FranceIX Route Server
65500:1013	Prepend 3x to FranceIX Route Server
65500:1021	Prepend 1x to FranceIX Private Peering
65500:1022	Prepend 2x to FranceIX Private Peering
65500:1023	Prepend 3x to FranceIX Private Peering
65500:1031	Prepend 1x to Appliwave
65500:1032	Prepend 2x to Appliwave
65500:1033	Prepend 3x to Appliwave
65500:1041	Prepend 1x to FNCIX RS
65500:1042	Prepend 2x to FNCIX RS

65500:1043	Prepend 3x to FNCIX RS
65500:1051	Prepend 1x to FNCIX Private Peering
65500:1052	Prepend 2x to FNCIX Private Peering
65500:1053	Prepend 3x to FNCIX Private Peering

Do not announce to Dyjix’s upstream or peering partners

You can remove the prefix announcement to Dyjix’s upstream or peering partners using BGP community described into “**Our upstreams and peering partners are designed as follow**” and replace the last number from “**9**” :

Community	Effect
65500:1009	Do not announce to Fiberway
65500:1019	Do not announce to FranceIX Route Server
65500:1029	Do not announce to FranceIX Private Peering
65500:1039	Do not announce to Appliwave
65500:1049	Do not announce to FNCIX RS
65500:1059	Do not announce to FNCIX Private Peering

Blackhole

Community	Effect
65535:666	Nullroute /32 IPv4 and /128 for IPv6

Graceful BGP session shutdown

Well-known BGP community GRACEFUL_SHUTDOWN (65535:0) to signal the graceful shutdown of paths has been introduced by the IETF. The purpose of this community is to reduce the amount of traffic lost when BGP peering sessions are about to be shut down deliberately, e.g. for planned maintenance.

Community	Effect
65535:0	Set local preference to 0 for graceful BGP session shutdown

BGP Bidirectional Forwarding Detection (BFD)

For customers who have a BGP session setup on a Layer 3 circuit with Dyjix, Dyjix offers the ability to run BGP Bidirectional Forwarding Detection (BFD).

BGP BFD tests the reachability of a peer and allows either side to take down a BGP session faster than the standard BGP default timers.

To enable BGP BFD you will need to configure it on your device.

Dyjix uses the following multiplier and millisecond interval for its default values:

Parameter	Time
Multiplier	3
Interval	333

To verify if your device supports BGP BFD, please consult with your hardware vendor.

IX. Support & Peering

Dyjix operates "NOC" support and 24/7 monitoring.
You will find the means of contact in the following table:

Service	E-mail	Phone
Network Operation Center	noc@dyjix.eu	+33 1 89 16 28 08 [3]
Support	support@dyjix.eu	+33 1 89 16 28 08 [2]
Abuse	abuse@dyjix.eu	+33 1 89 16 93 13
Peering	peering@dyjix.eu	+33 1 89 16 93 13